

IN THE CLAIMS

For the convenience of the Examiner, all pending claims of the present Application are shown below in numerical order whether or not an amendment has been made.

1. **(Currently Amended)** A method for detecting and removing malicious code from a computer system, comprising:

 determining an operating system of the computer system;

determining a memory scanning pattern specific to the determined operating system for scanning a memory of the computer system for malicious code;

 scanning the computer system for malicious code according to the memory scanning pattern, based on the determined operating system; and detecting the malicious code.

2. **(Currently Amended)** The method of claim 1, further comprising:
 removing detected the malicious code from the computer system.

3. **(Currently Amended)** The method of claim 1, further comprising displaying a message to a user identifying detected the malicious code.

4. **(Original)** The method of claim 1, further comprising displaying a message to a user indicating the presence of malicious code in the computer system.

5. **(Original)** The method of claim 2, wherein the removing step further comprises retrieving from a data file, information relating to the detected malicious code, including at least one command for restoring the computer system to a state that existed prior to modification by the malicious code and executing the at least one command for restoring the computer system to substantially a state that existed prior to modification by the malicious code.

6. **(Original)** The method of claim 5, wherein the data file is retrieved based on a command from the user.

7. **(Original)** The method of claim 1, wherein the scanning step further comprises scanning a memory of the computer system in accordance with a memory layout associated with the determined operating system.

8. **(Original)** The method of claim 1, wherein the scanning step comprises dividing memory locations of the computer system into a plurality of memory blocks and scanning predetermined memory blocks in accordance with the determined operating system.

9. **(Original)** The method of claim 6, wherein selected memory blocks are not scanned in accordance with the determined operating system.

10. **(Currently Amended)** A storage medium including computer executable code for detecting and removing malicious code from a computer system, comprising:
code for determining an operating system of the computer system;
code for determining a memory scanning pattern specific to the determined operating system for scanning a memory of the computer system for malicious code;
code for scanning the computer system for malicious code according to the memory scanning pattern; based on the determined operating system; and
code for detecting the malicious code.

11. **(Original)** The storage medium of claim 10, further comprising:
code for removing the malicious code from the computer system.

12. **(Original)** The storage medium of claim 10, further comprising code for displaying a message to a user identifying the malicious code.

13. **(Original)** The storage medium of claim 10, further comprising code for displaying a message to a user indicating that the malicious code is present on the computer system.

14. **(Previously Presented)** The storage medium of claim 11, wherein the code for removing the malicious code further comprises:

code for retrieving from a data file, information relating to the malicious code including at least one command for restoring the computer system to substantially a state that existed prior to modification by the malicious code and executing the at least one command for restoring the computer system to substantially a state that existed prior to modification by the malicious code after the message identifying the malicious code is displayed to the user.

15. **(Original)** The storage medium of claim 14, wherein the code for retrieving is implemented in response to a command from a user.

16. **(Original)** The storage medium of claim 10, wherein the code for scanning further comprises code for scanning a memory of the computer system according to a memory layout associated with the determined operating system.

17. **(Original)** The storage medium of claim 10, wherein the code for scanning further comprises code for dividing memory locations of the computer system into a plurality of memory blocks and scanning predetermined memory blocks in accordance with the determined operating system.

18. **(Previously Presented)** The storage medium of claim 17, wherein the code for scanning further comprises code for determining selected memory blocks that are not scanned in accordance with the determined operating system.

19. **(Currently Amended)** Software stored on a tangible computer-readable media for detecting and removing malicious code from a computer system, the computer system operable when executing the software to perform the following steps, comprising:

determining an operating system of the computer system;

determining a memory scanning pattern specific to the determined operating system for scanning a memory of the computer system for malicious code;

scanning the computer system for malicious code according to the memory scanning pattern; based on the determined operating system; and

detecting the malicious code.

20. **(Previously Presented)** The software of claim 19, further comprising the steps of:

removing the malicious code.

21. **(Previously Presented)** The software of claim 19, further comprising the steps of displaying a message to a user identifying the malicious code.

22. **(Previously Presented)** The software of claim 19, further comprising the steps of displaying a message indicating to a user that malicious code is present in the computer system.

23. **(Previously Presented)** The software of claim 20, wherein removing the malicious code further comprises:

retrieving from a data file, information relating to the malicious code including at least one command for restoring the computer system to a state that existed prior to modification by the malicious code and executing the at least one command for restoring the computer system to substantially a state that existed prior to modification by the malicious code.

24. **(Previously Presented)** The software of claim 23, wherein the data file is retrieved in response to a command from a user.

25. **(Previously Presented)** The software of claim 19, further comprising the steps of scanning a memory of the computer system in accordance with a memory layout associated with the determined operating system.

26. **(Previously Presented)** The software of claim 19, wherein the scanning further comprises dividing memory locations of the computer system into a plurality of memory blocks and scanning predetermined memory blocks in accordance with the determined operating system.

27. **(Previously Presented)** The software of claim 26, wherein the scanning further includes determining selected memory blocks that are not scanned, based on the determined operating system.

28. **(Currently Amended)** A system for detecting and removing malicious code from a computer system, comprising:

an identifying device adapted to determine an operating system of the computer system;

a determining device adapted to determine a memory scanning pattern specific to the determined operating system for scanning a memory of the computer system for malicious code;

a scanning device adapted to scan the computer system for malicious code according to the memory scanning pattern; based on the determined operating system; and

a code identifying device adapted to detect the malicious code.

29. **(Currently Amended)** The system of claim 28, wherein the memory scanning pattern identifies one or more portions of the memory that are unused by the determined operating system and indicates that the unused portions are to be left unscanned. further comprising: a code removal device adapted to remove the malicious code from the computer system.

30. **(Currently Amended)** The system of claim 28, wherein the memory scanning pattern optimizes scanning the computer system for malicious code by identifying portions of the memory that are unsusceptible to malicious code (“unsusceptible memory portions”) due to treatment of the unsusceptible memory portions by the determined operating system and indicates that the unsusceptible memory portions are to be left unscanned. further comprising a display device adapted to display a message to a user identifying the malicious code.

31. **(Currently Amended)** The system of claim 28, wherein the scanning device is adapted to scan the computer system for malicious code by searching for viral signatures in the memory.

further comprising a display device adapted to display a message indicating to a user that malicious code is present on the computer system.

32. **(Currently Amended)** The system of claim 29, wherein the code removal device further comprises:

a retrieving device adapted to retrieve, from a one or more restoration data file files specific to a detected malicious code, information relating to the malicious code including at least one command for restoring the computer system to a state that existed prior to modification by the detected malicious code; and

an execution device adapted to execute the at least one command for restoring the computer system to substantially the same state as it existed prior to modification by the detected malicious code.

33. **(Currently Amended)** The system of claim 32 28, wherein the memory scanning pattern identifies a memory layout specific to the determined operating system and uses the memory layout to identify portions of the memory that are unsusceptible to malicious code.

the data file is retrieved in response to a command from a user.

34. **(Original)** The system of claim 28, wherein the scanning device further scans a memory of the computer system in accordance with a memory layout associated with the determined operating system.

35. **(Original)** The system of claim 28, wherein the scanning device divides memory locations of the computer system into a plurality of memory blocks and scans predetermined memory blocks in accordance with the determined operating system.

36. **(Original)** The system of claim 35, wherein the scanning device does not scan selected memory blocks based on the determined operating system.